P.E.S. COLLEGE OF ENGINEERING

(AN AUTONOMOUS INSTITUTE)

CHH. SAMBHAJINAGAR-431002

Regular Winter Examination – 2025

Course: F.Y.M. Tech. Branch : CSE (Cyber Security) Semester : I
Subject Code & Name: MTPESCS103T Operating System Security

Max Marks: 60 Date: Duration: 3 Hr.

Answer Key

Q. 1	**Solve Any one of the following.**
A)	Describe the importance of security in multi-user operating systems. Answer Fundamental Pillars of Multi-User Security: Confidentiality (Privacy and Isolation), Integrity (System Protection), Availability (Fair Resource Allocation) (6 M) Major Threats in Multi-User Environments: Privilege Escalation, Information Leakage, Insider Threats (6 M)
B)	Explain how virtual memory contributes to process isolationandprotection. Answer The Concept of Private Address Spaces: Indirection, Isolation (4 M) Mechanisms of Protection: Access Control Bits (Permissions), Kernel vs. User Space Separation, Bounds Checking (4 M) Advanced Security Features: ASLR (Address Space Layout Randomization), Shared Memory with Control (4 M)
Q.2	**Solve Any one of the following.**
A)	Explain the Bell–LaPadula (BLP) model in detail. What areitsmain properties and security rules? Answer Introduction to BLP (3 M) The Main Properties and Security Rules: Simple Security Property (The "No Read Up" Rule), The $\star$-Property (Star Property) (The "No Write Down" Rule), Discretionary Security Property (3 M) The Tranquility Principle (3 M) Comparison with Biba (3 M)
B)	Define Authentication and Authorization. How are they differentand interrelated?

	Answer Definition of Authentication(3 M) Definition of Authorization(3 M) Key Differences(3 M) How They Are Interrelated(3 M)
Q. 3	**Solve Any one of the following.**
A)	Explain secure file operations and data sanitization techniques. Answer Secure File Operations: Atomic Operations, Access Control Validation, File Encryption at Rest, Secure Temporary Files (6 M) Data Sanitization Techniques: Overwriting (Clearing), Cryptographic Erasure (Crypto-Erase), Degaussing (Purging), Physical Destruction (6 M)
B)	What is tagged architecture? How does it enhance memoryprotection? Answer Definition of Tagged Architecture (3 M) The Tagging Mechanism: Data Field, Tag Field (3 M) Enhancing Memory Protection: Type Integrity, Prevention of Code Injection, Capability-Based Security, Detection of Uninitialized Memory (3 M) Comparison with Traditional Protection (3 M)
Q.4	**Solve Any one of the following.**
A)	What is fuzzing? Explain its types, working, and applicationsinvulnerability discovery. Answer Definition The Working Mechanism (4 M) Types of Fuzzing: Based on Input Generation, Based on Program Awareness (4 M) Applications in Vulnerability Discovery: Zero-Day Discovery, Protocol Testing, File Parser Security, Regression Testing (4 M)
B)	Write a detailed note on buffer overflow vulnerabilities. Answer:(2 M each) How a Buffer Overflow Works Common Types of Buffer Overflows Vulnerable Functions Impact of the Vulnerability Mitigation and Prevention

Q. 5	**Solve Any one of the following.**
A)	Explain how to minimize the attack surface of anoperatingsystem. Answer Introduction to Attack Surface: Goal, Core Principle (4 M) Strategic Minimization Techniques: Least Functionality (Service Hardening), Network Surface Reduction,Removal of Legacy Components, User and Privilege Minimization (4 M) Technical Hardening Features (4 M)
B)	Write a detailed note on security event logging anditsimportance. Answer Definition of Logging and Event Types(3 M) Types of Security Events Logged: Authentication Events, Privilege Changes, Object Access, System Changes, Network Activity (3 M) Importance of Security Event Logging: Intrusion Detection and Real-time Alerting, Forensic Investigation (Post-Incident Analysis), Regulatory Compliance, Accountability (Non-repudiation) (3 M) Best Practices for Secure Logging: Centralization, Immutable Logs, Time Synchronization, Verbosity Management (3 M)